Transmit Classical and Quantum Information Secretly

Li Yang(1) and Ling-An Wu(2)
(1)State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences, Beijing 100039,P. R. of China
(2)Institute of Physics, Chinese Academy of Sciences, Beijing 100086, China

Abstract This note presents a practical quantum cryptography protocol for transmitting classical and quantum information secretly and directly.

First, let's consider the transmission of classical message. The protocol is:

1. Alice prepares n bits for transmission:

$$a_1 a_2 \cdots a_n, \tag{1}$$

and chooses

$$\{\varphi_{Ai} | i = 1, 2, \cdots, n\} \tag{2}$$

randomly from a K-element set

$$\{\alpha_k = \frac{k\pi}{K}, k = 0, 1, \cdots, K-1\} \tag{3}$$

by means of local random number sources.

2. Alice prepares n single-photons, the i-th be in the state

$$|\Psi_i\rangle_{A0} = (a_i \oplus 1)|H\rangle + a_i|V\rangle, \tag{4}$$

where the $\oplus$ is the plus in F_2; then changes the polarization directions of photons separately and get

$$|\Psi_i\rangle_{A1} = (a_i \oplus 1)|\varphi_{Ai}\rangle + a_i|\varphi_{Ai} + \frac{\pi}{2}\rangle; \tag{5}$$

then sends these photons to Bob one by one.

3. Bob chooses

$$\{\varphi_{Bi}|i=1,2,\cdots,n\} \tag{6}$$

randomly independently from the K-element set (3) by means of local random number source, and changes the polarization directions of photons separately as below:

$$|\Psi_i\rangle_{B1}=(a_i\oplus 1)|\varphi_{Ai}+\varphi_{Bi}\rangle+a_i|\varphi_{Ai}+\varphi_{Bi}+\frac{\pi}{2}\rangle; \tag{7}$$

then Bob sends back these photons to Alice.

4. Alice changes the polarization direction of the photons again and gets:

$$|\Psi_i\rangle_{A2}=(a_i\oplus 1)|\varphi_{Bi}\rangle+a_i|\varphi_{Bi}+\frac{\pi}{2}\rangle; \tag{8}$$

then sends them to Bob again.

5. Bob changes the polarization direction of the photons again and gets:

$$|\Psi_i\rangle_{B2}=(a_i\oplus 1)|H\rangle+a_i|V\rangle; \tag{9}$$

then measures the photons in bases $\{|H\rangle,|V\rangle\}$ one by one and gets the message (1).

Now let's consider the secret transmission of quantum information. It is obviously that the changes needed are trivial. The protocol becomes:

1. Alice chooses n qubits for transmission:

$$|\varphi_1\rangle,|\varphi_2\rangle,\cdots,|\varphi_n\rangle, \tag{10}$$

and chooses

$$\{\varphi_{Ai}|i=1,2,\cdots,n\} \tag{11}$$

randomly from a K-element set

$$\{\alpha_k=\frac{k\pi}{K},k=0,1,\cdots,K-1\} \tag{12}$$

by means of local random number sources.

2. Alice prepares n single-photons, the i-th be in the state

$$|\Psi_i\rangle_{A1}=|\varphi_i+\varphi_{Ai}\rangle; \tag{13}$$

sends these photons to Bob one by one.

3. Bob chooses

$$\{\varphi_{Bi}|i=1,2,\cdots,n\} \tag{14}$$

randomly from the K-element set (3) by means of local random number source, and changes the polarization directions of photons separately as below:

$$|\Psi_i\rangle_{B1}=|\varphi_i+\varphi_{Ai}+\varphi_{Bi}\rangle; \tag{15}$$

then sends back these photons to Alice.

4. Alice changes the polarization direction of the photons again and gets:

$$|\Psi_i\rangle_{A2}=|\varphi_i+\varphi_{Bi}\rangle; \tag{16}$$

then sends them to Bob again.

5. Bob changes the polarization direction of the photons again and gets:

$$|\Psi_i\rangle_{B2}=|\varphi_i\rangle; \tag{17}$$

then he gets the message (10).

Because $\varphi_{Ai},\varphi_{Bi}$are chosen from set (3) randomly and independently, Eve cannot get any information from simple intercept/resend attack. Unfortunately, These two protocols cannot defend man in the middle(of quantum channel only) attack, even though there is an authenticated classical channel. To overcome this problem, Alice and Bob need to share $\{\varphi_{Ci},i=1,\cdots,n\}$secretly before communication. Then, For example, the second protocol becomes:

1. Alice chooses n qubits for transmission:

$$|\varphi_1\rangle,|\varphi_2\rangle,\cdots,|\varphi_n\rangle, \tag{18}$$

and chooses

$$\{\varphi_{Ai}|i=1,2,\cdots,n\} \tag{19}$$

randomly from a K-element set

$$\{\alpha_k=\frac{k\pi}{K},k=0,1,\cdots,K-1\} \tag{20}$$

by means of local random number sources.

2. Alice prepares n single-photons, the i-th be in the state

$$|\Psi_i\rangle_{A1}=|\varphi_{Ci}+\varphi_i+\varphi_{Ai}\rangle; \tag{21}$$

then sends these photons to Bob one by one.

3. Bob chooses

$$\{\varphi_{Bi}|i=1,2,\cdots,n\} \tag{22}$$

randomly from the K-element set (3) by means of local random number source, and changes the polarization directions of photons separately:

$$|\Psi_i\rangle_{B1}=|\varphi_{Ci}+\varphi_i+\varphi_{Ai}+\varphi_{Bi}\rangle; \tag{23}$$

then sends them back to Alice.

4. Alice changes the polarization direction of the photons again and gets:

$$|\Psi_i\rangle_{A2}=|\varphi_{Ci}+\varphi_i+\varphi_{Bi}\rangle; \tag{24}$$

then sends them to Bob again.

5. Bob changes the polarization direction of the photons again and gets:

$$|\Psi_i\rangle_{B2}=|\varphi_i\rangle; \tag{25}$$

then he gets the message (18).

The authentication information $\{\varphi_{Ci}, i=1,\cdots,n\}$ can be used repeatedly under the protection of continuously changed local random numbers $\{\varphi_{Ai},\varphi_{Bi}, i=1,\cdots,n\}$.

[1]C.H.Bennett, et al.,J.Cryptography(1992)5:3-28